Fall 2012

# CEG 4420/6420-01: Host Computer Security

Prabhaker Mateti
*Wright State University - Main Campus*, prabhaker.mateti@wright.edu


# CEG 4420/6420: Host Computer Security Syllabus

**TBD Catalog Description:** Introduction to security issues arising primarily from computer networks. Topics include node and service authentication, address spoofing, hijacking, SYN floods, sniffing, routing tricks, and privacy of data en route. Buffer overruns and other exploitation of software development errors. Hardening of operating systems. Intrusion detection. Firewalls. Ethics. **Prerequisites:** CEG 4350

## Source Material

**Home Page**
http://www.cs.wright.edu/people/faculty/pmateti/Courses/429 Please visit the home page for announcements, and info on notes. There is no required text book this term.

**Simson Garfinkel, Gene Spafford, and Alan Schwartz**
Practical Unix and Internet Security, 3rd edition (2003), O'Reilly & Associates; ISBN: 0596003234. A *recommended* text book. Errata Previous Editions: http://www.oreilly.com/catalog/puis/errata/
http://proquest.safaribooksonline.com.ezproxy.libraries.wright.edu:2048/ book/ networking/ security/0596003234

**Elizabeth D. Zwicky, Simon Cooper, and D. Brent Chapman**
Building Internet Firewalls, Second Edition O'Reilly Media, Inc., 2000. A *recommended* text book.
http://proquest.safaribooksonline.com.ezproxy.libraries.wright.edu:2048/ book/networking/firewalls/1565928717

**Charles P.Pfleeger, Shari Lawrence Pfleeger,**
Security in Computing, Fourth Edition, Prentice Hall, 2006, ISBN-10: 0-13-239077-9. A *recommended* text book.
http://proquest.safaribooksonline.com.ezproxy.libraries. wright.edu: 2048/ book/networking/security/0132390779

## Attendance

Full attendance is expected.

## Course Content

Lab work is a significant part of this course. The ordering of lectures, in contrast to the course content topics listed below, is largely due to this influence.

The topics are described at some length because they may be too unfamiliar to you. The numbers in parens are a rough estimate of the number of (75-minute) lectures on each topic.

### System Administration (3)

The initial boot can be a significant source of insecurity.

The sequence of events from initial power-on cold booting to shut down of a computer system. Standard Unix processes: `init`, `getty`, `inetd`, `rpc.*`, etc. User Authentication: /etc/passwd, /etc/shadow files. So-called one time passwords. Semi-permanently assigned password, and a response token generated by credit-card-sized electronic authenticators.

Introduction to network setup. TCP/IP refresher. Configuring properly. Hardening an OS. Root kits. Backdoors. Honey pots.

### Well Known Security Breaches (1)

The most famous and most recent incidents. The Internet Worm, Nov 2, 1988. Current events. Hacker v. attacker v. cracker.

### Virus, Worms, and Trojan Horses (2)

The structure of a computer virus. Anti-virus programs. Worms. Trojans. Preventive techniques.

## Secure Software Development (2)

Buffer Overflow Exploitation. Software development techniques that are resistant to bug exploits. At the high-level, code structure, least privilege, and narrow interfaces, and at the low-level, checking for buffer overruns, being ultra careful in writing setuid programs, untrusted paths, race conditions, environment, etc. Type-safety, assertions and invariants.

## TCP/IP Exploits (2)

Modern operating systems are internally organized as a networked collection of servers. Node Authentication is nearly absent in most LANs. A machine merely declares what its IP address is and its neighbors simply believe it. Simple checks that relate the hardware address (such as Ethernet address) with IP address and with symbolic host names have always been available but are only now beginning to see widespread use. But these are easy to defeat.

Domain Name Service (DNS). NIS. Router protocols (RIP). Service and node authentication. Probing a Host for Weakness. Remote Trojans. Causing service denials. Denial of Service Attacks. Distributed coordinated attacks. Sniffing. Spoofing.

## Firewalls (3)

At one time (circa 1994), a firewall was a gateway/router. Today (2000) there are some commercial products that label themselves as ``firewalls" that run on PCs with Windows98/NT that have a modem but no network interface cards. A security system is run on a machine that has no ordinary user accounts and runs a stripped down, and hardened version of the OS kernel. The non-specialist computer community uses the term ``firewall" as being a network security system, whereas most firewall products are packet filters and proxy servers now nicely wrapped in GUI and frequently bundled with network hardware.

Packet filters. Circuit (or connection) gateways. An address translating firewall. Stateful inspection in a packet filter. Bastion host. Proxy servers, application gateways. Setting up a Linux PC as a Packet Filtering Router

## Detection and Documentation of Intrusions (2)

The security system should have an always-on logging facility that logs all attempts to connect to the protected LAN, attempts to connect to the Internet, and problems with firewall software. The size of the audit records produced in a day of normal use can be large. Manual review of this much data by even a skilled system administrator would take too long and become tedious enough to miss crucial aberrations.

Intrusion Detection Systems (IDS). Security audit. Tripwire. Nessus. SAINT.

## Security Standards (1)

Survey of a few government originated standards. Cryptography. Fortezza Crypto Cards. The Orange Book. Secure computing architectures and levels A1 (most secure) through D (least).

## Applied Cryptography (1)

Internet is based mostly on TCP/IP version 4. TCP/IPv4 was designed at a time when security threats were relatively unknown. Network packets are unencrypted. Any attacker can copy the packets with a typical PC.

IP version 6 (IPv6) is the successor to IPv4. There is no IPv5. Adopting IPv6 implies retooling the network infrastructure. Trade literature trumpets IPv6 as ``the blueprint for 21st century e-commerce." IPv6 increases the IP address size from 32 bits to 128 bits, has simpler auto-configuration of addresses, has more efficient forwarding, and can request `real-time' quality of service. More importantly for us, it has extensions to support authentication, data integrity, and data confidentiality.

Secure shell. Secure Socket Layer (SSL). Virtual Private Networks (VPN). IPv6.

## Ethical and Legal Issues (2)

We will have guest lectures on legal and ethical issues. We will discuss the written decision of U.S. District Court, United States of America, Appellee, v. Robert Tappan Morris, Defendant-Appellant. We will discuss papers such as ``Why Hackers Do The Things They Do", by Ira S. Winkler, ICSA News, June 96.

## Exams 20 + 30%

There will be two exams contributing 20% and 30% to the final grade. The mid term is scheduled around the sixth week, and the final during the exam week as set by the Registrar.

## Laboratory Experiments 12*4%

The laboratory experiments contribute 48% to the final grade. I expect to give 12 experiments worth 4% each. Lab reports must be submitted by midnight on the due date posted. I will accept up to two lab reports late but each within 48 hours. *The subject matter of these experiments is included in the exams.*

All lab work must be, with a couple of exceptions, conducted within the Operating Systems and Internet Security (OSIS) Lab. No other WSU facilities are allowed. It is required that you sign our statement of ethics.

In this course, a lab rarely involves writing your own programs. It generally will require you to build an executable after suitable reconfiguration using tools such as make. The source code tree will be given to you. The code is in C/C++, Java, or in (one or two cases) ASM code.

Most experiments are to be performed by the student individually with a few that are best learned when there is a pair of students. These labs must be work done *solely by you (and your partner)*, except for the parts I provided you with.

## Discussion 2%

Active participation in the group discussions is expected. TBD

## Homework Assignments

There are no homework assignments to be turned in.

## CEG 6420

Students enrolled in CEG 629 are required to do an additional task. This quarter the task is to (i) learn and write a technical summary in a few pages on one of the topics below, (ii) sketch a new lab experiment based on that topic, and (iii) carry out that experiment and submit a lab report as usual. Your article and lab experiment should look like one of those already included in the course. If a topic beyond this list interests you, let us consider it.

1. Linux Intrusion Detection System (LIDS).
2. Intrusion Detection and Logging using Linux Snort
3. A Linux-based Honey Pot.
4. Hardening a well-known Linux distribution
5. Virus construction kits.
6. Distributed Denial of Service (DDoS).

---